PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-101035
(43)Date of publication of application : 13.04.1999

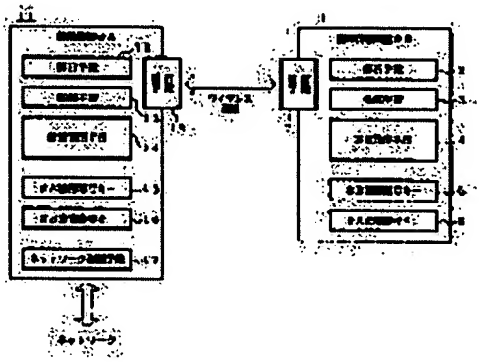
(51)Int.Cl. E05B 49/00
H04L 9/32

(21)Application number : 09-264138
(22)Date of filing : 29.09.1997

(71)Applicant : PFU LTD
(72)Inventor : YAMAMOTO YOJI

(54) LOCK DEVICE SYSTEM AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enhance safety by encoding/transmitting an individual locking code changing each time when a device ID is received from a portable terminal, and comparing it with former transmission data by again receiving/decoding an encoded signal from the portable terminal.
SOLUTION: Analyzing means 2 and 12 respectively analyze data transmitted from a lock device 11 and a portable information terminal 1. Secret code keys 5 and 15 and public code keys 6 and 16 respectively decode encoded data. When the portable information terminal 1 transmits a device proper ID, the lock device 11 confirms the ID, and encodes/transmits an individual locking code containing a time stamp changing each time by a public code key of the portable information terminal 1. Next, the portable information terminal 1 decodes a received signal, and encodes/transmits it again by the public code key of the lock device 11. The lock device 11 decodes the received signal, and discriminates whether or not it coincides with the former transmission content, and also discriminates whether or not the time stamp is within a prescribed time. Therefore, safety is enhanced, and a lock can be set and opened.



LEGAL STATUS

[Date of request for examination] 22.01.2001
[Date of sending the examiner's decision of rejection] 11.05.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－101035

(43)公開日　平成11年(1999)４月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｋ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｂ
			６７５Ｂ

審査請求　未請求　請求項の数８　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－264138

(22)出願日　平成９年(1997)９月29日

(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２

(72)発明者　山本　洋史
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内

(74)代理人　弁理士　岡田　守弘

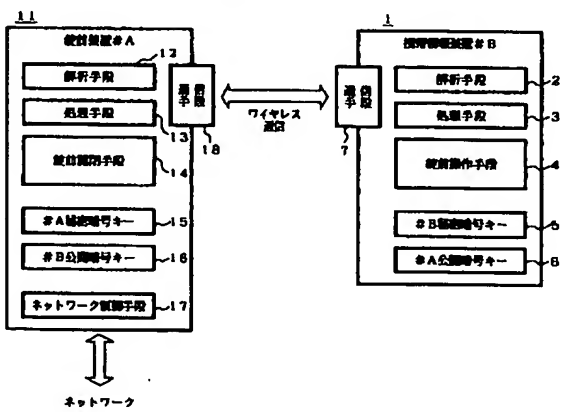
(54)【発明の名称】　錠前装置システムおよび記録媒体

(57)【要約】

【課題】　本発明は、錠前を施錠あるいは開錠する錠前装置システムおよび記録媒体に関し、錠前装置と操作用の携帯情報装置との間で暗号化技術を使って安全性を高めることを目的とする。

【解決手段】　自装置の装置ＩＤを施錠装置に送信する手段と、送信に対応して施錠装置から返信されてきたデータについて自装置の秘密暗号キーで復号した後、錠前装置の公開暗号キーで暗号化して送信する手段とからなる装置と、装置から受信した装置ＩＤが予め登録されていた装置ＩＤと一致したときに装置ＩＤに一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して上記装置に返信する手段と、返信したことに対応して装置から送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと個別施錠コードとが一致したときに指定された施錠あるいは開錠を行う手段とからなる施錠装置とを備えた錠前装置システムである。

本発明のシステム構成図



1

【特許請求の範囲】

【請求項１】錠前を施錠あるいは開錠する錠前装置システムにおいて、

自装置の装置ＩＤを施錠装置に送信する手段と、上記送信に対応して施錠装置から返信されてきたデータについて自装置の秘密暗号キーで復号した後、錠前装置の公開暗号キーで暗号化して送信する手段とからなる装置と、

上記装置から受信した装置ＩＤが予め登録されていた装置ＩＤと一致したときに装置ＩＤに一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して上記装置に返信する手段と、上記返信したことに対応して上記装置から送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと上記個別施錠コードとが一致したときに指定された施錠あるいは開錠を行う手段とからなる施錠装置とを備えた錠前装置システム。

【請求項２】上記毎回変化する個別施錠コードとして、時刻あるいは時刻と乱数でランダムに作成したコードを組み合わせた情報としたことを特徴とする請求項１記載の施錠装置システム。

【請求項３】上記復号したデータと上記個別施錠コードとが一致し、かつ当該個別施錠コード中の時刻と現時刻との差が所定時間以内のときに指定された施錠あるいは開錠を行うことを特徴とする請求項１あるいは請求２記載の施錠装置システム。

【請求項４】自装置の公開暗号キーおよび錠前装置ＩＤを管理装置に送信する手段と、錠前装置から送信されてきたデータを自装置の秘密暗号キーを用いて復号化した錠前装置の公開暗号キーを登録する手段とを設けた装置と、

上記装置から送信されてきた装置の公開暗号キーおよび錠前装置ＩＤと当該錠前装置ＩＤのキー登録プログラムを錠前装置ＩＤの公開暗号キーで暗号化して錠前装置に送信する手段を設けた管理装置と、

上記管理装置から送信されてきたデータを自身の秘密暗号キーで復号化したキー登録プログラムおよび装置の公開暗号キーを登録する手段と、登録した装置の公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して上記装置に送信する手段とを設けた錠前装置とを備え、続いて請求項１ないし請求項３記載のいずれかの処理を実行することを特徴とする錠前装置システム。

【請求項５】自装置の公開暗号キーを錠前装置に送信する手段と、錠前装置から送信されてきたデータを自装置の秘密暗号キーを用いて復号化して錠前装置の公開暗号キーを登録する手段とを設けた装置と、

上記装置から送信されてきた装置の公開暗号キーを登録すると共に当該公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して上記装置に送信する手段とを設けた錠前装置とを備え、続いて請求項１ないし請求項３記載のいずれかの処理を実行することを特徴とする錠前装置システム。

2

【請求項６】上記登録した公開暗号キーに使用回数あるいは使用期間の制限を付与して当該制限を越えたときに自己消滅するプログラムを付与したことを特徴とする請求項４あるいは請求項５記載の錠前装置システム。

【請求項７】錠前装置の施錠したときに当該錠前装置の公開暗号キーを用いて錠前開閉制御プログラムを暗号化した後に装置の公開暗号キーを用いて暗号化して装置に送信すると共に錠前開閉制御プログラムを消去する手段と、開錠するときに装置から送信されてきたデータを自錠前装置の秘密暗号キーを用いて復号した錠前開閉制御プログラムをインストールして開錠する手段とを設けた錠前装置と、

上記施錠したときに錠前装置から送信されてきたデータを保持する手段と、開錠するときに上記保持したデータを自装置の秘密暗号キーを用いて復号して上記錠前装置に送信する手段とを設けた装置とを備え、上記施錠および開錠の直前に請求項１ないし請求項３記載のいずれかの処理をそれぞれ実行することを特徴とする錠前装置システム。

【請求項８】コンピュータを動作させ、

自装置の装置ＩＤを施錠装置に送信する手段と、上記送信に対応して施錠装置から返信されてきたデータについて自装置の秘密暗号キーで復号した後、錠前装置の公開暗号キーで暗号化して送信する手段として機能させる、装置に格納するプログラムと、

上記装置から受信した装置ＩＤが予め登録されていた装置ＩＤと一致したときに装置ＩＤに一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して上記装置に返信する手段と、上記返信したことに対応して上記装置から送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと上記個別施錠コードとが一致したときに指定された施錠あるいは開錠を行う手段として機能させる、施錠装置に格納するプログラムとのいずれか、あるいは両者を記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、錠前を施錠あるいは開錠する錠前装置システムおよび記録媒体に関するものである。

【０００２】

【従来の技術】従来、キーレスエントリと称して、ワイヤレス通信による錠前機構が数多く提供されるようになった。

【０００３】

【発明が解決しようとする課題】しかし、従来の装置では、ワイヤレス通信情報を傍受された場合に錠前としての安全性に欠けるという問題があった。

【０００４】本発明は、これらの問題を解決するため、

錠前装置と操作用の携帯情報装置との間で暗号化技術を使って安全性を高めることを目的としている。

【０００５】

【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、携帯端末装置（装置）１は、秘密暗号キーおよび公開暗号キーを用いて錠前装置１１の施錠あるいは開錠を行うものである。

【０００６】錠前装置１１は、秘密暗号キーおよび公開暗号キーを用いて装置１との間でデータの送受信して錠前を施錠あるいは開錠するものである。次に、動作を説明する。

【０００７】装置（携帯情報装置）１が自装置の装置ＩＤを施錠装置１１に送信し、施錠装置１１が受信した装置ＩＤについて予め登録されていた装置ＩＤと一致したときに装置ＩＤに一緒に登録されている装置の公開暗号キーを用いて毎回変化する個別施錠コードを暗号化して装置１に返信し、装置１が返信されてきたデータについて自装置の秘密暗号キーで復号した後に、錠前装置の公開暗号キーで暗号化して送信し、錠前装置１１が送信されてきたデータを錠前装置の秘密暗号キーで復号したデータと個別施錠コードとが一致したときに指定された施錠あるいは開錠を行うようにしている（処理（Ａ）とする）。

【０００８】この際、毎回変化する個別施錠コードとして、時刻あるいは時刻と乱数でランダムに作成したコードを組み合わせた情報とするようにしている。また、復号したデータと個別施錠コードとが一致し、かつ個別施錠コード中の時刻と現時刻との差が所定時間以内のときに指定された施錠あるいは開錠を行うようにしている。

【０００９】また、装置１が管理装置に公開暗号キーおよび錠前装置ＩＤを送信し、管理装置が送信されてきた装置の公開暗号キーおよび錠前装置ＩＤと錠前装置ＩＤのキー登録プログラムを錠前装置ＩＤの公開暗号キーで暗号化して錠前装置１１に送信し、錠前装置１１が送信されてきたデータを自身の秘密暗号キーで復号化したキー登録プログラムおよび装置の公開暗号キーを登録すると共に登録した装置の公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して装置１に送信し、装置１が送信されてきたデータを自装置の秘密暗号キーを用いて復号化して錠前装置の公開暗号キーを登録するようにしている。そして、上記処理（Ａ）を実行するようにしている。

【００１０】また、装置１が自装置の公開暗号キーを錠前装置１１に送信し、錠前装置１１が送信されてきた装置の公開暗号キーを登録すると共に公開暗号キーを用いて自錠前装置の公開暗号キーを暗号化して装置１に送信し、装置１が送信されてきたデータを自装置の秘密暗号キーを用いて復号化して錠前装置の公開暗号キーを登録するようにしている。そして、上記処理（Ａ）を実行するようにしている。

【００１１】この際、登録した公開暗号キーに使用回数あるいは使用期間の制限を付与して制限を越えたときに自己消滅するプログラムを付与するようにしている。また、錠前装置１１が施錠したときに錠前装置の公開暗号キーを用いて錠前開閉制御プログラムを暗号化した後に装置の公開暗号キーを用いて暗号化して装置１に送信すると共に錠前開閉制御プログラムを消去し、装置１が送信されてきたデータを保持し、開錠するときに保持したデータを自装置の秘密暗号キーを用いて復号して錠前装置１１に送信し、錠前装置１１が送信されてきたデータを自錠前装置の秘密暗号キーを用いて復号した錠前開閉制御プログラムをインストールして開錠するようにしている。この際、施錠および開錠の直前に上記処理（Ａ）を実行するようにしている。

【００１２】従って、錠前装置１１と装置（携帯情報端末）１との間で暗号化技術を使って安全性を高めて、錠前装置１１の施錠あるいは開錠を行うことが可能となる。

【００１３】

【発明の実施の形態】次に、図１から図５を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１４】図１は、本発明のシステム構成図を示す。ここで、図示外の記録媒体あるいは外部記憶装置であるハードディスク装置から読み出したプログラム、またはセンタのはハードディスク装置から回線を介して転送されてきたプログラムを主記憶にローディングして起動し、以下に説明する各種処理を行うものである。

【００１５】図１において、携帯情報装置（装置）１は、ここでは以下の説明を簡単にするために装置１と記載し、施錠装置１１の施錠あるいは開錠を暗号技術（秘密暗号キーおよび公開暗号キーを用いた例えば公知のＤＥＳ技術）を用いて行うものであって、解析手段２、処理手段３、錠前操作手段４、秘密暗号キー５、公開暗号キー６などから構成されるものである。

【００１６】解析手段２は、錠前装置１１などから送信されてきたデータを解析し、該当する処理を実行させるものである。処理手段３は、解析手段２によって解析された結果をもとに各種処理を行うものである。

【００１７】錠前操作手段４は、錠前を施錠あるいは開錠操作などを指示するものである。秘密暗号キー５および公開暗号キー６は、ＤＥＳ技術などで用いる秘密暗号キーおよび公開暗号キーであって、秘密暗号キーを用いて暗号化されたデータは公開暗号キーで復号化でき、逆に公開暗号キーを用いて暗号化されたデータは秘密暗号キーで復号化できるという性質を持つものである。

【００１８】通信手段７は、ワイヤレス通信で施錠装置１１との間でデータの送受信を行うものである。施錠装置１１は、図示外の錠前を施錠したり開錠したりなどするものであって、解析手段２、処理手段３、錠前開閉手

段４、秘密暗号キー１５、公開暗号キー１６、ネットワーク制御手段１７、および通信手段１８などから構成されるものである。

【００１９】解析手段１２は、携帯情報装置１などから送信されてきたデータを解析し、該当する処理を実行させるものである。処理手段１３は、解析手段１２によって解析された結果をもとに各種処理を行うものである。

【００２０】錠前開閉手段１４は、錠前を施錠あるいは開錠したりするものであって、キー登録プログラムによって実行するものである。秘密暗号キー１５および公開暗号キー１６は、ＤＥＳ技術などで用いる秘密暗号キーおよび公開暗号キーであって、秘密暗号キーを用いて暗号化されたデータは公開暗号キーで復号化でき、逆に公開暗号キーを用いて暗号化されたデータは秘密暗号キーで復号化できるという性質を持つものである。

【００２１】ネットワーク制御手段１７は、ネットワークを介して管理装置や他の携帯情報装置１との間でデータの授受を行うものである。通信手段１８は、ワイヤレス通信で携帯情報装置１との間でデータの送受信を行うものである。

【００２２】次に、図２のフローチャートに示す順序に従い図１の構成の動作を詳細に説明する。図２は、本発明の動作説明フローチャート（その１）を示す。ここで、携帯情報端末１を＃Ｂ、錠前装置１１を＃Ａと説明を簡単にするために記述する。

【００２３】図２において、Ｓ１は、携帯情報端末１が錠前の操作を開始し、＃Ｂ（携帯情報端末１を表す）の装置固有ＩＤを送信する。Ｓ２は、錠前装置１１がＳ１で送信されたデータを受信し、受信したＩＤの装置の公開暗号キーが＃Ａ（錠前装置１１を表す）内に登録されているか確認する。

【００２４】Ｓ３は、登録されているか判別する。ＹＥＳの場合には、Ｓ４に進む。ＮＯの場合には、登録されていないと判明したので、エラーとして終了する。Ｓ４は、＃Ｂの公開暗号キーで毎回変化する個別施錠コード（タイムスタンプを含む）情報を暗号化する。これは、毎回変化する個別施錠コードとして、現在の時刻を用い、これを暗号化する。

【００２５】Ｓ５は、Ｓ４で暗号化した情報（データ）を送信する。Ｓ６は、Ｓ５で送信された情報を受信する。Ｓ７は、＃Ｂ秘密暗号キーで受信情報を復号化する。これにより、Ｓ４で暗号化した元の個別施錠コードが復号されたこととなる。

【００２６】Ｓ８は、復号した情報を＃Ａ公開暗号キーで暗号化する。これは、Ｓ７で復号された個別施錠コードを、＃Ａ公開暗号キー（施錠装置１１の公開暗号キー）で暗号化する。

【００２７】Ｓ９は、Ｓ８で暗号化した情報を送信する。Ｓ１０は、Ｓ９で送信された情報を受信する。Ｓ１１は、＃Ａ秘密暗号キーで受信情報を復号化し、元の個別施錠コードを復号する。

【００２８】Ｓ１２は、送信内容と一致か判別する。これは、Ｓ１１で受信情報を復号した情報（元の個別施錠コード）と、Ｓ４の個別施錠コードとが一致するか判別する。ＹＥＳの場合には、＃Ｂの認証がＯＫとしてＳ１３で、更にタイムスタンプが所定時間以内か判別する。これは、Ｓ１１で復号化したときに含まれているＳ４で含ませたタイムスタンプと現在の時刻とを比較し、その差が所定時間以内か判別する。ＹＥＳの場合には、所定時間以内で正当性が高いとしてＳ１４に進む。ＮＯの場合には、正当性が低いとして施錠／開錠を認めず、終了する。

【００２９】Ｓ１４は、施錠状態か判別する。ＹＥＳの場合には、Ｓ１５で開錠し、終了する。ＮＯの場合には、Ｓ１６で施錠し、終了する。以上によって、装置＃Ｂが装置固有ＩＤを施錠装置＃Ａに送信し、施錠装置＃Ａが装置＃Ｂの公開暗号キーで個別施錠コードとタイムスタンプを暗号化して装置＃Ｂに送信し、装置＃Ｂが装置＃Ｂの秘密暗号キーで復号し、復号した情報を施錠装置＃Ａの公開暗号キーで暗号化して送信し、施錠装置＃Ａが施錠装置＃Ａの秘密暗号キーで復号化して個別施錠コードと一致したときに、更に復号化したタイムスタンプの経過時刻が所定時間以内のときに装置＃ＢのＯＫとし、施錠あるいは開錠を行うことにより、装置＃Ｂと施錠装置＃Ａが暗号技術を用いて相互に通信して施錠装置＃Ａが装置＃Ｂの認証ＯＫとなったときに初めて施錠あるいは開錠を行い、暗号技術を合理的に使い安全性を高めることが可能となった。ここで、Ｓ１からＳ１６（あるいはＳ１からＳ１３）までの処理を処理（Ａ）としてこれを基本動作と記述し、後述する図３、図４、図５で該当する個所で実行する。

【００３０】図３は、本発明の動作説明フローチャート（その２）を示す。ここで、携帯情報端末１を＃Ｃ、錠前装置１１を＃Ａと説明を簡単にするために記述する。図３において、Ｓ２１は、錠前装置＃Ａを使いたいとし、＃Ｃ公開暗号キーを管理者へ渡す（あるいは送信する）。

【００３１】Ｓ２２は、錠前装置＃Ａ管理者（管理装置）が＃Ａのキー登録プログラム、＃Ｃ公開暗号キー、＃Ａ使用許可回数／期間をパックにした情報を、＃Ａ公開暗号キーで暗号化する。

【００３２】Ｓ２３は、暗号化情報をネットワーク経由で錠前装置＃Ａに送信する。Ｓ２４は、錠前装置＃ＡがＳ２３で送信された情報を受信する。Ｓ２５は、＃Ａ秘密暗号キーで復号化する。

【００３３】Ｓ２６は、復号化した＃Ａのキー登録プログラムを起動する。Ｓ２７は、指定された利用回数／利用期間条件を持ち、＃Ａに＃Ｃ公開暗号キーが登録される。これにより、錠前装置＃Ａには、利用回数／利用期間条件を付与した装置＃Ｃの公開暗号キーが登録される

こととなる。

【００３４】Ｓ２８は、＃Ｃ公開暗号キーにより＃Ａ公開暗号キーを暗号化して＃Ｃに送信する。Ｓ２９は、Ｓ２８で送信された情報を、装置＃Ｃが受信する。

【００３５】Ｓ３０は、Ｓ２９で受信した情報を、＃Ｃ秘密暗号キーで復号化する。これにより、施錠装置＃Ａの公開暗号キーが復号されることとなる。Ｓ３１は、＃Ａ公開暗号キーを装置に登録する。

【００３６】Ｓ３２は、基本動作と同様に施錠操作を行う（既述した図２のＳ１ないしＳ１６で装置＃Ｃの認証および施錠／開錠を行う）。また、Ｓ３３は、施錠装置＃Ａが図２の既述した基本動作と同様に施錠動作をＳ３２に対応して行う。

【００３７】Ｓ３４は、使用回数／期限を越えたか判別する。ＹＥＳの場合には、Ｓ３５で登録されている＃Ｃ公開暗号キーの登録を抹消し、以降施錠／開錠できないようにし、もし盗用されてもいつまでも継続されることを防止することが可能となる。一方、Ｓ３４のＮＯの場合には、Ｓ３３で戻り繰り返す。

【００３８】以上によって、装置＃Ｃが自身の公開暗号キーおよび操作したい施錠装置＃Ａを管理装置（管理者）に通知し、管理装置（管理者）がキー登録プログラム、＃Ｃ公開暗号キー、使用回数／期間を暗号化して施錠装置＃Ａに送信し、施錠装置＃Ａがキー登録プログラムを起動し、指定された使用回数／期間を付与した＃Ｃ公開暗号キーを登録すると共に、＃Ｃ公開暗号キーで＃Ａ公開暗号キーを暗号化した送信し、装置＃Ｃが＃Ｃ秘密暗号キーで復号し、復号した＃Ａ公開暗号キーを登録し、基本動作（既述した図２のＳ１からＳ１６）により施錠あるいは開錠を行うことが可能となる。そして、施錠装置＃Ａに登録した＃Ｃ公開暗号キーに付与されているの使用回数／期限が越えたときに抹消し、再登録を促し、継続した盗用を防止することが可能となる。

【００３９】図４は、本発明の動作説明フローチャート（その３）を示す。ここで、携帯情報端末１を＃Ｄ、錠前装置１１を＃Ａと説明を簡単にするために記述する。図４において、Ｓ４１は、携帯情報端末１が錠前の操作を開始し、＃Ｄ公開暗号キーを送信する。

【００４０】Ｓ４２は、錠前装置１１がＳ４１で送信された＃Ｄ公開暗号キーを受信する。Ｓ４３は、未登録装置の操作許可モードか判別する。ＹＥＳの場合には、Ｓ４４に進む。ＮＯの場合には、終了する。

【００４１】Ｓ４４は、一定の条件（使用回数／期限）により自己消滅するプログラムを内包した＃Ａ公開暗号キーを＃Ｄ公開暗号キーで暗号化する。Ｓ４５は、暗号化した情報を送信する。

【００４２】Ｓ４６は、Ｓ４５で送信された情報を、装置＃Ｄが受信する。Ｓ４７は、＃Ｄ秘密暗号キーで受信情報を復号化する。これにより、Ｓ４４で暗号化した元のプログラムを内包した＃Ａ公開暗号キーを復元できる。

【００４３】Ｓ４８は、復号した＃Ａ公開暗号キーを登録する。Ｓ４９は、基本動作と同様に施錠操作する。これは、既述した図２のＳ１、Ｓ６ないしＳ９を実行する。そして、Ｓ５０に進む。

【００４４】Ｓ５０は、使用回数／期限を越えたか判別する。ＹＥＳの場合には、Ｓ５１で＃Ａ公開暗号キーが内包されているプログラムにより自己消滅し、終了する。ＮＯの場合には、Ｓ４９を繰り返し、施錠あるいは開錠を繰り返す。

【００４５】また、Ｓ５２は、施錠装置＃Ａが＃Ｄ公開暗号キーを使用回数／期限条件付きで登録する。Ｓ５３は、基本動作と同様に施錠動作する。これは、既述した図２のＳ２ないしＳ５、Ｓ１０からＳ１６を実行する。そして、Ｓ５４に進む。

【００４６】Ｓ５４は、使用回数／期限を越えたか判別する。ＹＥＳの場合には、Ｓ５５で＃Ｄ公開暗号キーを内包するプログラムが登録を抹消し、終了する。ＮＯの場合には、Ｓ５３を繰り返し、施錠あるいは開錠を繰り返す。

【００４７】以上によって、装置＃Ｄが＃Ｄ公開暗号キーを施錠装置＃Ａに送信し、施錠装置＃Ａが装置＃Ｄの公開暗号キーで使用回数／期限付きで消滅するプログラムを内包させた＃Ａ公開暗号キーを暗号化して送信し、装置＃Ｄが装置＃Ｄの秘密暗号キーで復号し、復号した＃Ａ公開暗号キーを登録し、図２で既述したようにして施錠あるいは開錠を行い、登録した公開暗号キー使用回数／期限を越えたときに自動消滅させ、再登録を促し、安全性を高めることが可能となる。

【００４８】図５は、本発明の動作説明フローチャート（その４）を示す。ここで、携帯情報端末１を＃Ｂ、錠前装置１１を＃Ａと説明を簡単にするために記述する。図５において、Ｓ６１は、基本動作の（Ａ）までの動作（図２のＳ１ないしＳ１３）までの動作を実行する。

【００４９】Ｓ６２は、施錠状態か判別する。ＹＥＳの場合には、施錠状態であるため終了する。ＮＯの場合には、Ｓ６３に進む。Ｓ６３は、施錠する。

【００５０】Ｓ６４は、施錠装置の開閉制御プログラムをまず＃Ａ公開暗号キーで暗号化後、その情報をさらに＃Ｂ公開暗号キーで暗号化する。Ｓ６５は、暗号化した情報を送信する。そして、Ｓ６５’で錠前装置の開閉制御プログラムを消去する。

【００５１】Ｓ６６は、Ｓ６５で送信された情報を、装置＃Ｂが受信し、受信情報Ｐを保持する。Ｓ６７は、装置＃Ｂが錠を開錠したいと指定する。

【００５２】Ｓ６８は、Ｓ６１と同様に、基本動作の（Ａ）までの動作（図２のＳ１ないしＳ１３）までの動作を実行する。Ｓ６９は、錠前装置＃Ａが情報Ｐの送信要求を通知する。

【００５３】Ｓ７０は、装置＃Ｂが要求を受信の後、情

報Ｐを＃Ｂ秘密暗号キーで復号化し、Ｓ６４で＃Ａ秘密暗号キーで暗号化された情報に戻す。Ｓ７１は、Ｓ７０で復号化した情報Ｐ’を送信する。そして、Ｓ７５で情報Ｐ（Ｐ’）を消去する。

【００５４】Ｓ７２は、錠前装置＃ＡがＳ７１で送信された情報Ｐ’を受信し、＃Ａ秘密暗号キーで復号し、元の開閉制御プログラムに戻す。Ｓ７３は、復号化した錠前機構制御プログラムを装置にインストールする。これにより、Ｓ６５’で消去した錠前装置の開閉制御プログラムが復元されたこととなる。

【００５５】Ｓ７４は、開錠する。以上によって、装置＃Ｂが施錠装置＃Ａを施錠した後、施錠装置＃Ａが開閉制御プログラムを＃Ａ公開暗号キーで暗号化し、更に＃Ｂ公開暗号キーで二重に暗号化した装置＃Ｄに送信し、装置＃Ｄが情報Ｐを保持する。そして、開錠時に、保持した情報Ｐを装置＃Ｄが秘密暗号キーで復号してこれを施錠装置＃Ｄに送信し、施錠装置＃Ｄが秘密暗号キーで復号して元の開閉制御プロウラムに戻し、インストールして開錠を行うことにより、施錠時に錠前装置＃Ｄに開閉制御プログラムを抹消し、開錠時に装置＃Ｄが秘密暗号キーで復号して施錠装置＃Ｄに送信しこれを更に秘密暗号キーで復号して元の開閉制御プログラムに戻してインストールして開錠し、安全性を決めた高くすることが可能となる。

【００５６】

【発明の効果】以上説明したように、本発明によれば、錠前装置１１と装置１との間で秘密暗号キーおよび公開暗号キーを使って情報や開閉制御プログラムのやり取りを行い、装置１の認証を行った後に施錠あるいは開錠を行う構成を採用しているため、安全性を高めて錠前装置１１の施錠あるいは開錠を行うことができると共に、登録した公開暗号キーに使用回数／期限の制限を付与してこれを越えたときに抹消し、再登録を促し、更に安全性を高めることができる。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

【図２】本発明の動作説明フローチャート（その１）である。

【図３】本発明の動作説明フローチャート（その２）である。

【図４】本発明の動作説明フローチャート（その３）である。

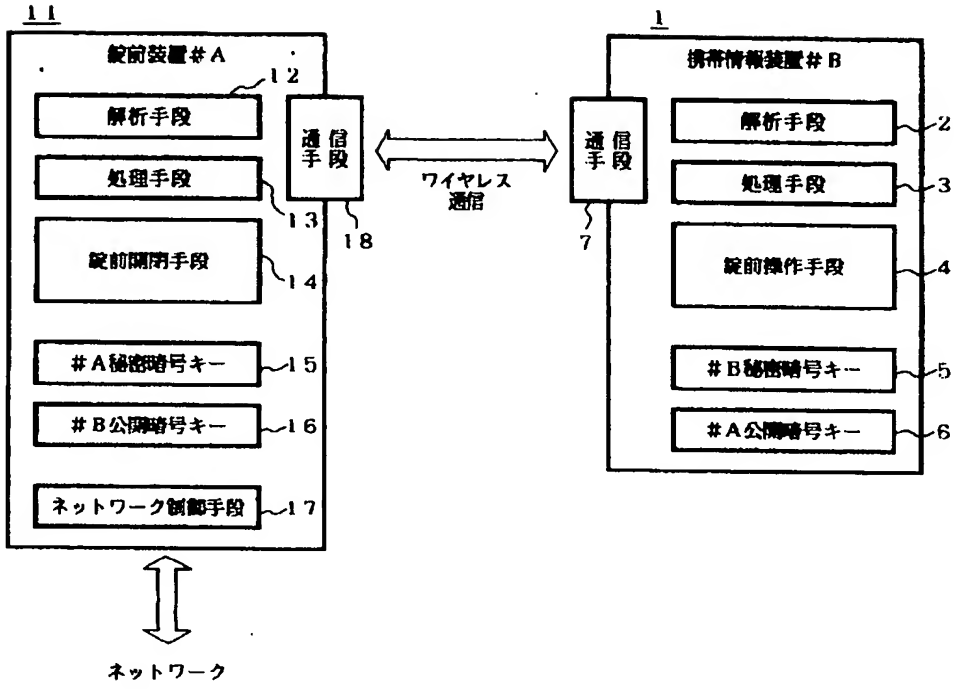
【図５】本発明の動作説明フローチャート（その４）である。

【符号の説明】

１：装置（携帯情報装置）
２、１２：解析手段
３、１３：処理手段
４：錠前操作手段
５、１５：秘密暗号キー
６、１６：公開暗号キー
７、１８：通信手段
１１：錠前装置
１４：錠前開閉手段
１７：ネットワーク制御手段

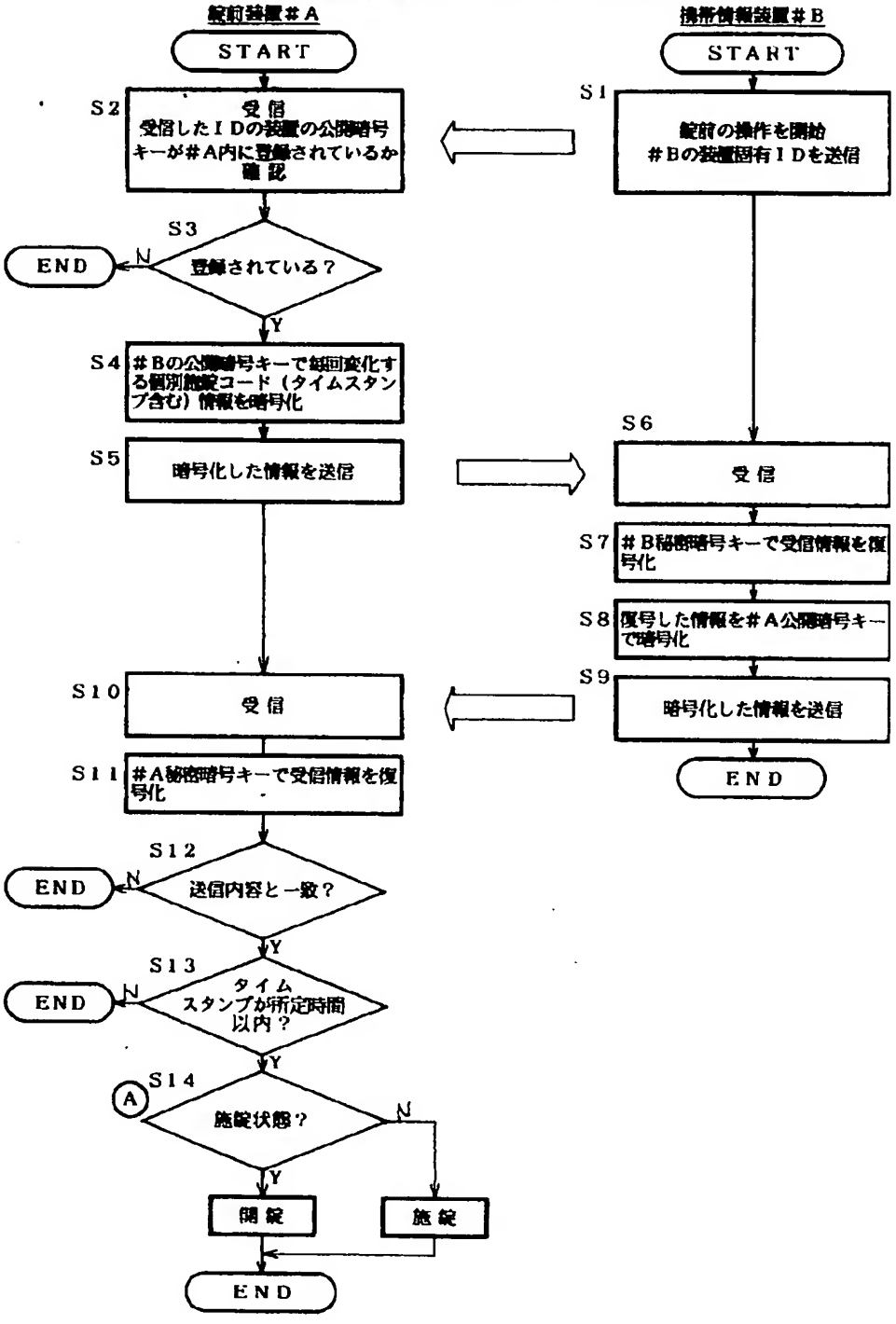
【図１】

本発明のシステム構成図



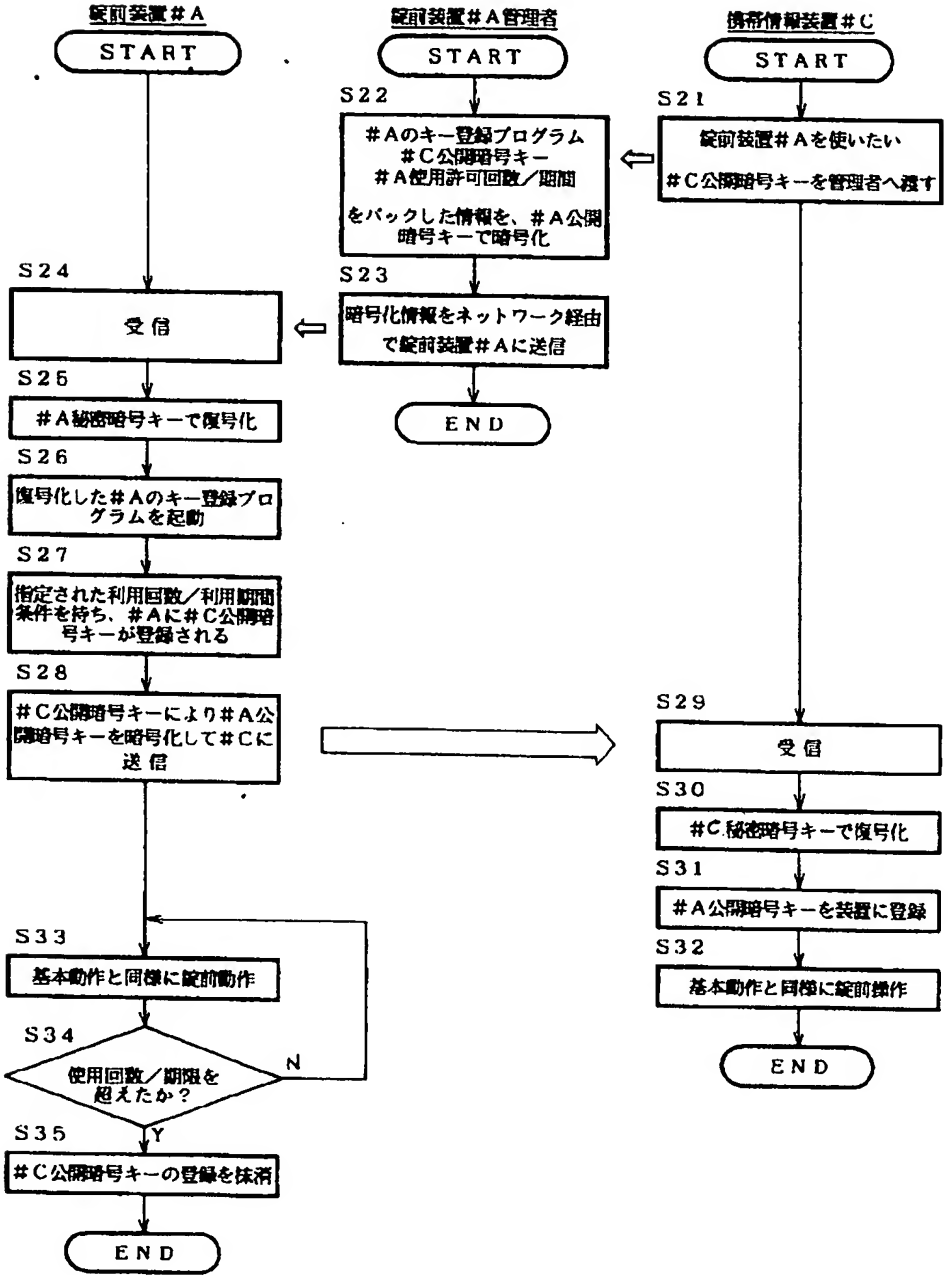
【図2】

本発明の動作説明フローチャート（その1）



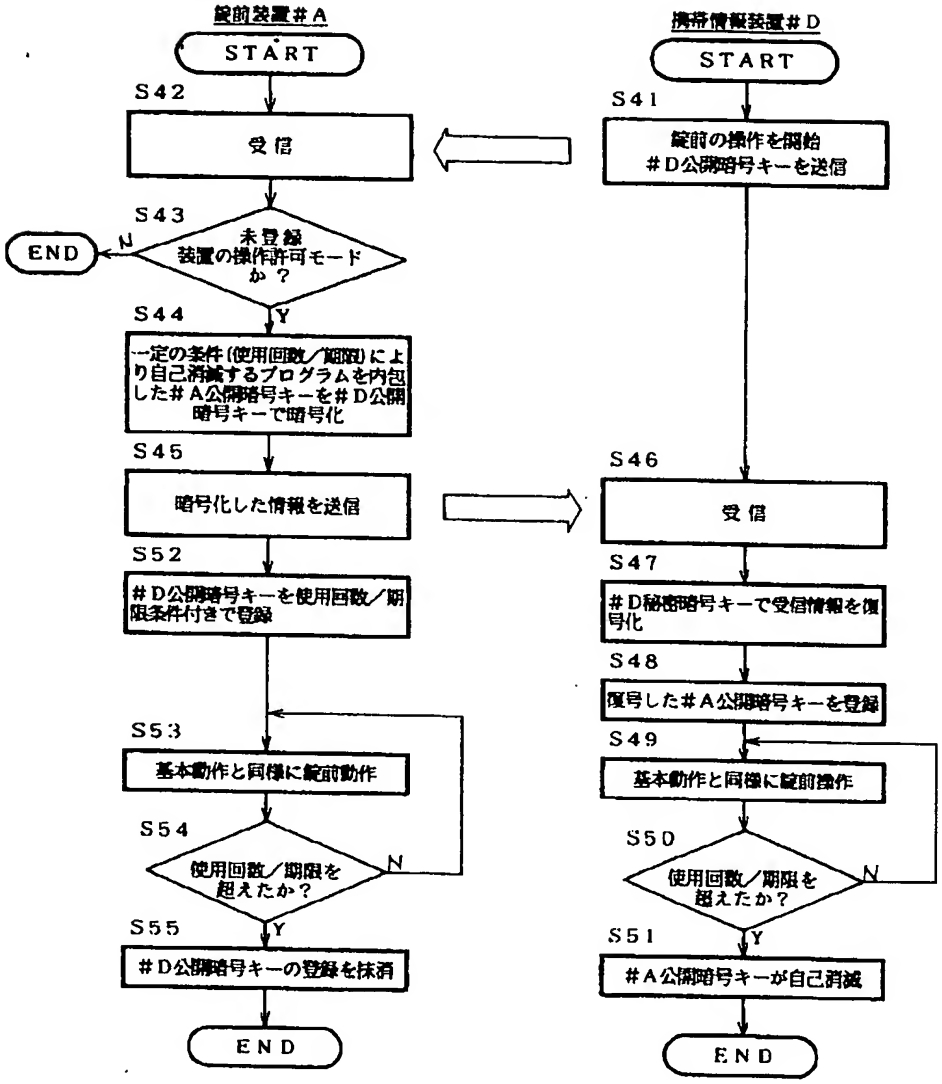
【図3】

本発明の動作説明フローチャート（その2）



【図４】

本発明の動作説明フローチャート(その3)



【図５】

本発明の動作説明フローチャート(その4)